JOURNAL OF NUMBER THEORY 33, 95–100 (1989)

Sets That Determine Integer-Valued Polynomials

ROBERT GILMER*

Department of Mathematics, Florida State University, Tallahassee, Florida 32306-3027

Communicated by H. Zassenhaus

Received July 18, 1988; revised November 29, 1988

As usual, let Z and Q, respectively, denote the sets of integers and rational numbers, and let $D = \mathrm{Int}(Z)$ be the ring of integer-valued polynomials on Z. Thus $\mathrm{Int}(Z) = \{f(X) \in Q[X] \mid f(Z) \subseteq Z\}$. The study of $\mathrm{Int}(Z)$ and related rings stems from algebraic number theory, and has its origin in consecutive 1919 papers of Ostrowski [9] and Polya [10] of the same title. In particular, Polya showed that $\mathrm{Int}(Z)$ is free as an additive abelian group and that $\{f_n(X)\}_{n=0}^{\infty}$ is a basis for $\mathrm{Int}(Z)$, where $f_0(X) = 1$ and where, for $n > 1$,

$$f_n(X) = \binom{X}{n} = \frac{X(X-1)\cdots(X-n+1)}{n!}.$$

More recently, Brizolis [1, Th. 2] showed that D is a two-dimensional Prüfer domain, and using the notation $I(a)$ to denote the set $\{f(a) \mid f \in I\}$ for an ideal I of D and for $a \in Z$, Brizolis also showed [1, Th. S] that finitely generated ideals I, J of D are equal if and only $I(a) = J(a)$ for each $a \in Z$; this latter property of D has subsequently been referred to as the *strong Skolem property* [4], reflecting the fact that Skolem [12] proved the result in the case where $J = D$. (For generalization to the case of $\mathrm{Int}(E)$, where E is a Dedekind domain with finite residue fields, see [8, 3].) Using the strong Skolem property of D, Gilmer and Smith showed in [5, Th. 4.2] that each finitely generated ideal of D can be generated by two elements. Murad Özaydin has pointed out (personal communication) that a comment in the last sentence preceding the statement of Proposition 2.5 of [5] is clearly in error; the comment would imply, for example, that if $f(X) \in Q[X]$ is such that $f(a) \in Z$ for infinitely many integers a, then $f \in D$, whereas $f = X/2$ provides an obvious counterexample to this assertion. In this connection, Özaydin asked the following question:

* Research partially supported by NSF Grant DMS-8501003.

0022-314X/89 $3.00

641/33/1-7

(*) *What subsets S of Z determine integer-valued polynomials on Z, in the sense that D contains each polynomial $f(X) \in Q[X]$ such that $f(S) \subseteq Z$?*

In this note we provide an answer to question (*) in Theorem 2, and we subsequently use Theorem 2 to extend Propositions 2.4–2.6 of [5]; these three propositions are related to the strong Skolem property, and they fall generally in the area of asking for conditions under which an element or a finitely generated ideal of D is determined by its set of values on a subset of Z. To facilitate the statement of results, we say that a subset S of Z is *prime-power complete* if S contains a complete set of residues modulo q for each prime power $q \in Z^+$. Our first result is an elementary lemma whose proof we omit.

LEMMA 1. *Suppose I is an ideal of the ring R and let $\{r_\alpha\}_{\alpha \in A}$ be a complete set of residues of I in R. If $f(X) \in R[X]$ is such that $f(r_\alpha) \in I$ for each $\alpha \in A$, then $f(R) \subseteq I$.*

THEOREM 2. *For a subset S of Z, the following conditions are equivalent.*

(1) *S determines the set of integer-valued polynomials on Z.*

(2) *S is prime-power complete.*

Proof. To prove that (1) implies (2), we establish the contrapositive. Thus, assume that there exists a prime power $q = p^t \in Z^+$ such that S does not contain a complete set of residues modulo q, and choose i with $0 \leqslant i \leqslant q-1$ such that no element of S is congruent to i modulo q. Let $A_q(X) = X(X-1)\cdots(X-q+1)$. If $n = [q/p] + [q/p^2] + \cdots = p^{t-1} + p^{t-2} + \cdots + 1 = (p^t - 1)/(p-1) = (q-1)/(p-1)$, where $[\cdot]$ denotes the greatest integer function, then it is known [10, p. 106] or [2, Lem. 1] that $A_q(y) \in p^n Z$ for each $y \in Z$, while there exists $y_0 \in Z$ (for example, $y_0 = q$, where $A_q(y_0) = q!$ [11, p. 143]) such that $A_q(y_0) \notin p^{n+1}Z$. Let $B(X) = A_q(X-i)$. Since $B(Z) = A_q(Z)$, it follows that $B(Z) \subseteq p^n Z$, but $B(Z) \not\subseteq p^{n+1}Z$. Let $C(X) = B(X)/(X-i) = (X-i-1)(X-i-2)\cdots(X-i-q+1)$. If $s \in S$, then $p^n \mid B(s) = (s-i)(s-i-1)\cdots(s-i-q+1)$ and since, by assumption, $p^t \nmid (s-i)$, it follows that p^{n-t+1} divides $(s-i-1)\cdots(s-i-q+1) = C(s)$. Hence if $f(X) = C(X)/p^{n-t+1}$, then $f(X) \in Q[X]$ and $f(S) \subseteq Z$. However, $f(i) = (-1)^{q-1}(q-1)!/p^{n-t+1}$, and the highest power of p dividing $(q-1)!$ is $p^n/q = p^{n-t}$. Consequently, $f(i) \notin Z$ and $f(X) \notin D$ so that (1) also fails for S.

Conversely, assume that S is prime-power complete and that $f(X) \in Q[X]$ satisfies $f(S) \subseteq Z$. Write $f(X) = g(X)/n$, where $g(X) \in Z[X]$ and $n \in Z^+$. We know that $g(S) \subseteq nZ$ and we wish to show that $g(Z) \subseteq nZ$. It suffices to show that $g(Z) \subseteq qZ$ for each prime-power divisor q of n, and

this statement follows from Lemma 1 since $g(S) \subseteq qZ$ and S contains a complete set of residues modulo q. This completes the proof of Theorem 2.

Let T be a cofinite subset of Z—that is, $Z \setminus T$ is finite. Proposition 2.4 of [5] shows that if $F(X), G(X) \in D$ are such that $F(a) \in G(a)Z$ for each $a \in T$, then $F(X) \in G(X)D$. Using Theorem 2, we show in Theorem 4 and Proposition 7 that the prime-power complete sets are precisely the subsets T of Z for which this statement is valid. Again the proof of Theorem 4 uses a basic lemma.

LEMMA 3. *Suppose $\alpha(X) \in Q(X)$ is such that $\alpha(S) \subseteq Z$ for an infinite subset S of Z. Then $\alpha(X) \in Q[X]$.*

Proof. Write $\alpha(X) = f(X)/g(X)$, where $f(X), g(X) \in Q[X]$. By the division algorithm in $Q[X]$, we can write $f(X) = g(X)\,q(X) + r(X)$, where $r(X) = 0$ or $\deg r(X) < \deg g(X)$. Hence if $n \in Z^+$ is such that $nq(X) \in Z[X]$, then $n\alpha(X) = nq(X) + \alpha_1(X)$, where $\alpha_1(X) = nr(X)/g(X)$. If T is the finite subset of S consisting of those element $s \in S$ such that $g(s) \neq 0$, then $\alpha_1(T) \subseteq Z$. Moreover, if $\alpha_1(X) \in Q[X]$, then $\alpha(X)$ is also in $Q[X]$. Hence, without loss of generality we assume that $f(X) = 0$ or $\deg f(X) < \deg g(X)$; in this case we show, in fact, that $\alpha(X) = f(X) = 0$. Because S is infinite, there exists a sequence $\{s_i\}_{i=1}^{\infty} \subseteq S$ such that $\lim_{i \to \infty} s_i$ is $+\infty$ or $-\infty$. In either case, $\lim_{i \to \infty} \alpha(s_i) = 0$ since $f(X) = 0$ or $\deg f(X) < \deg g(X)$. Because each $\alpha(s_i)$ is an integer, it follows that $\alpha(s_i)$, and hence $f(s_i)$, is 0 for i sufficiently large. Therefore $f(X) = \alpha(X) = 0$ and $\alpha(X) \in Q[X]$, as we wished to show.

THEOREM 4. *Suppose S is a prime-power complete subset of Z. If $F(X), G(X) \in D$ are such that $F(s) \in G(s)Z$ for each $s \in S$, then $F(X) \in G(X)D$.*

Proof. Since the set S is infinite, the conclusion of the theorem is valid if $G(X) = 0$. If $G(X) \neq 0$, if $\alpha(X) = F(X)/G(X)$, and if T is the infinite subset of S on which $G(X)$ does not vanish, then $\alpha(T) \subseteq Z$, so Lemma 3 implies that $\alpha(X) \in Q[X]$. Theorem 2 then implies that $\alpha(X) \in D$, and hence $F(X) \in G(X)D$, as asserted.

Theorem 5 and Corollary 6 represent analogues of Propositions 2.5 and 2.6 of [5]. Corollary 6 follows immediately from Theorem 5. The proof of Theorem 5 is similar to that of Proposition 2.5 (replace the reference to Proposition 2.4 by the reference to Theorem 4), and hence is omitted.

THEOREM 5. *Suppose S is a prime-power complete subset of Z. If I is a finitely generated ideal of D and $f(X) \in D$ is such that $f(s) \in I(s)$ for each $s \in S$, then $f(X) \in I$.*

COROLLARY 6. *Suppose S is a prime-power complete subset of Z. If I and J are finitely generated ideals of D such that $I(s) = J(s)$ for each $s \in S$, then $I = J$.*

We remark that the conclusion of neither Theorem 5 nor Corollary 6 is valid, even for $S = Z$, if the assumption that I is finitely generated is omitted. For example, Brizolis [1, Example 2] shows that there exist (non-finitely generated) maximal ideals M of D such that $M(n) = Z$ for each $n \in Z$.

The final result of the paper, Proposition 7, shows that the converse of each of the last three results is also valid.

PROPOSITION 7. *Suppose S is a subset of Z that is not prime-power complete.*

(1) *There exist $F(X), G(X) \in D$ such that $F(s) \in G(s)Z$ for each $s \in S$, but $F(X) \notin G(X)D$.*

(2) *There exist $f(X) \in D$ and a finitely generated ideal I of D such that $f(s) \in I(s)$ for each $s \in S$, but $f(X) \notin I$.*

(3) *There exist finitely generated I, J of D such that $I(s) = J(s)$ for each $s \in S$, but $I \neq J$.*

Proof. By Theorem 2, there exists $\alpha(X) \in Q[X] \setminus D$ such that $\alpha(S) \subseteq Z$. We write $\alpha(X) = g(X)/n$, where $g(X) \in Z[X]$ and $n \in Z^+$. Then in (1), we can take $F(X) = g(X)$ and $G(X) = n$. In (2), we take $f(X) = g(X)$ and $I = nD$, and in (3), we take $I = nD$ and $J = (g(X), n)D$. This completes the proof of Proposition 7.

We remark that Theorem 2 extends to the case of a Dedekind domain with finite residue fields (see the Appendix). That is, if E is a Dedekind domain with quotient field K and with finite residue fields, then a subset S of E determines the integer-valued polynomials on E in the sense that $\mathrm{Int}(E)$ contains each element $f(X) \in K[X]$ such that $f(S) \subseteq E$ if and only if S contains a complete set of residues modulo each power of each maximal ideal of E. On the other hand, Theorems 4 and 5 and Corollary 6 do not extend to this more general context. For example, if F is a finite field with q elements and if $E = F[[Y]]$, then the polynomial $X^q - X + 1 \in E[X]$ assumes only unit values on elements of E, but is not itself a unit of $\mathrm{Int}(E)$.

APPENDIX

We include here a proof that Theorem 2 extends to the case of a Dedekind domain with finite residue fields. Thus, let E be a Dedekind domain with finite residue fields and with quotient field K. Say that a

subset S of E *determines the integer-valued polynomials on* E if $\mathrm{Int}(E)$ contains each polynomial $f(X) \in K[X]$ such that $f(S) \subseteq E$, and say that S is *prime-power complete* if S contains a complete set of residues of P^k in E for each non-zero proper prime ideal P of E and for each positive integer k.

THEOREM 8. *With notation and hypothesis as above, the following conditions are equivalent:*

(1) *S determines the integer-valued polynomials on E.*

(2) *S is prime-power complete.*

Proof. (2) $\Rightarrow$ (1): Suppose S is prime-power complete and $f(X) \in K[X]$ is such that $f(S) \subseteq E$. We write $f(X) = g(X)/c$, where $g(X) \in E[X]$ and $c \in E \setminus (0)$. Then $g(S) \subseteq cE$ and we wish to show that $g(E) \subseteq cE$. Let $cE = Q_1 \cap \cdots \cap Q_n$ be a representation of cE as an intersection of ideals Q_i that are powers of maximal ideals of E. It suffices to show that $g(E) \subseteq Q_i$ for each i, and this follows from the fact that $g(S) \subseteq Q_i$ and S contains a complete set of residues modulo Q_i.

$\sim(2) \Rightarrow \sim(1)$: Suppose S is not prime-power complete and let $P \in \mathrm{MaxSpec}(E)$, $k \in Z^+$ be such that S does not contain a complete set of residues of P^k in E. Let $\{P_\alpha\}_{\alpha \in A} = \mathrm{MaxSpec}(E) \setminus \{P\}$, let v be a normed valuation associated with E_P, and let $t \in E$ be such that $v(t) = 1$ (hence $t \in P \setminus P^2$). Suppose $|(E/P)| = q$ and that $\{u_0 = 0, u_1, \ldots, u_{q-1}\}$ is a complete set of residues of P in E. We set $s_0 = u_0 = 0$ and for $n > 0$ with q-adic expansion $n = a_0 + a_1 q + \cdots + a_r q^r$, let $s_n = u_{a_0} + u_{a_1} t + \cdots + u_{a_r} t^r$. Let $h = q^k$. Then $\{s_i\}_{i=0}^{h-1}$ is a complete set of residues of P^k in E. Moreover, if $A(X) = \prod_{i=0}^{h-1} (X - s_i)$, then $A(X) \in E[X]$ and the following statements (i) and (ii) are known: (i) $A(E_P) \subseteq t^m E_P$, where $m = (h-1)/(q-1)$, and (ii) $v(A(t^k)) = m$ so that, in particular, $A(E_P) \not\subseteq t^{m+1} E_P$. Choose j with $0 \leqslant j \leqslant h-1$ such that no element of S is congruent to s_j modulo P^k. We write $A(X) = XB(X)$. (ii) implies that $A(t^k) = t^m u$, where u is a unit of E_P, so $B(t^k) = t^{m-k} u$. Let $C(X) = B(X - s_j)$. For any $s \in S$, we have $A(s - s_j) = (s - s_j)\, B(s - s_j) = (s - s_j)\, C(s)$, so $m \leqslant v(A(s - s_j)) = v(s - s_j) + v(C(s)) \leqslant k - 1 + v(C(s))$, and hence $v(C(s)) \geqslant m - k + 1$. Let $t^{m-k+1} E = P^{m-k+1} P_1^{e_1} \cdots P_w^{e_w}$ be the prime factorization of $t^{m-k+1} E$ in E and choose $y \in P_1^{e_1} \cdots P_w^{e_w} \setminus P$. We show that $D(X) = yC(X)/t^{m-k+1} \in K[X]$ is such that $D(S) \subseteq E$ but $D(E) \not\subseteq E$. To see that $D(E) \not\subseteq E$, we need only observe that $D(t^k + s_j) = yC(t^k + s_j)/t^{m-k+1} = yB(t^k)/t^{m-k+1} = yut^{m-k}/t^{m-k+1} = yu/t \notin E_P$, and hence $D(t^k + s_j) \notin E$. On the other hand, if $s \in S$, then $D(s) = yC(s)/t^{m-k+1} \in E_P$ since $v(C(s)) \geqslant m - k + 1$. Moreover, if $\alpha \in A$ and if v_α is a normed valuation associated with E_{P_α}, then by choice of y, $v_\alpha(y/t^{m-k+1}) \geqslant 0$ so that $v_\alpha(D(s)) = v_\alpha(C(s)) + v_\alpha(y/t^{m-k+1}) \geqslant 0$ as well. Consequently, $D(s)$ belongs to each E_{P_α}, and hence $D(s) \in E_P \cap (\bigcap_{\alpha \in A} E_{P_\alpha}) = E$. This completes the proof.

REFERENCES

1. D. BRIZOLIS, A theorem on ideals in rings of integer-valued polynomials, *Comm. Algebra* **7** (1979), 1065–1077.
2. J.-L. CHABERT, Anneaux de "polynomes à valeurs entières et anneaux de Fatou," *Bull. Soc. Math. France* **99** (1971), 273–283.
3. J.-L. CHABERT, Un anneaux de Prüfer, *J. Algebra* **107** (1987), 1–16.
4. J.-L. CHABERT, Ideaux de polynomes et ideaux de valeurs, *manuscr. math.* **60** (1988), 277–298.
5. R. GILMER AND W. W. SMITH, Finitely generated ideals of the ring of integer-valued polynomials, *J. Algebra* **81** (1983), 150–164.
6. H. GUNJI AND D. L. MCQUILLAN, On a class of ideals in an algebraic number field, *J. Number Theory* **2** (1970), 207–222.
7. H. GUNJI AND D. L. MCQUILLAN, On rings with a certain divisibility property, *Michigan Math. J.* **22** (1975), 289–299.
8. D. L. MCQUILLAN, On Prüfer domains of polynomials, *J. Reine Angew. Math.* **358** (1985), 162–178.
9. A. OSTROWSKI, Ueber ganzwertige Polynome in algebraischen Zahlkörpern, *J. Reine Angew. Math.* **149** (1919), 117–124.
10. G. POLYA, Ueber ganzwertige polynome in algebraischen Zahlkörpern, *J. Reine Angew. Math.* **149** (1919), 97–116.
11. J. ROTMAN, "An Introduction to the Theory of Groups," Allyn & Bacon, Boston, MA, 1984.
12. TH. SKOLEM, Ein Satz über ganzwertige Polynome, *Norske Vid. Selsk.* (*Trondheim*) **9** (1936), 111–113.